物理端口IP访问列表配置命令

目 录

第 1 章 配置物理端口IP 访问列表命令 1
1.1 基于物理端口的IP访问列表配置命令 1
1.1.1 deny 1
1.1.2 ip access-group 3
1.1.3 ip access-list 4
1.1.4 permit 5
1.1.5 show ip access-list 7

第1章　配置物理端口IP 访问列表命令

1.1　基于物理端口的IP访问列表配置命令

访问列表配置命令有：

- deny
- ip access-group
- ip access-list
- permit
- show ip access-list

1.1.1　deny

在 IP 访问列表配置模式中可使用此命令配置禁止规则，要从 IP 访问列表中删除 deny 规则，在命令前加 no 前缀。

deny source [*source-mask*]

no deny source [*source-mask*]

deny protocol source source-mask destination destination-mask [**tos** tos]

no deny protocol source source-mask destination destination-mask [**tos** tos]

对于互联网控制报文协议(ICMP)，也可以使用以下句法：

deny icmp source source-mask destination destination-mask [icmp-type] [**tos** tos]

对于 Internet 组管理协议(IGMP)，可以使用以下句法：

deny igmp source source-mask destination destination-mask [igmp-type] [**tos** tos]

对于 TCP，可以使用以下句法：

deny tcp source source-mask [operator port] destination destination-mask [operator port] [**tos** tos]

对于数据报协议(UDP)，可以使用以下句法：

deny udp source source-mask [operator port] destination destination-mask [operator port] [**tos** tos]

参数

参数	参数说明
protocol	协议名字或IP协议号。它可以是关键字icmp、igmp、igrp、ip、ospf、tcp或udp，也可以是表IP协议号的0到255的一个整数。为了匹配任何Internet协议(包括ICMP、TCP和UDP)使用关键字ip。某些协议允许进一步限定，如下描述。
source	源网络或主机号。有两种方法指定源：32位二进制数，用四个点隔开的十进制数表示。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
source-mask	源地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
destination	目标网络或主机号。有两种方法指定： 使用四个点隔开的十进制数表示的32位二进制数。 使用关键字any作为0.0.0.0 0.0.0.0的目标和目标掩码的缩写。
destination-mask	目标地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的目标地址和目标地址掩码缩写。
tos *tos*	(可选) 数据包可以使用服务层过滤。使用数字0－15指定。
icmp-type	(可选)ICMP包可由ICMP报文类型过滤。类型是数字0到255。
igmp-type	(可选)IGMP包可由IGMP报文类型或报文名过滤。 类型是0到15的数字。
operator	(可选)比较源或目标端口。操作包括eq(等于)。如果操作符放在source和source-mask之后，那么它必须匹配这个源端口。如果操作符放在destination和destination-mask之后，那么它必须匹配目标端口。
port	(可选)TCP或UDP端口的十进制数字或名称。端口号是一个0到65535的数字。

命令模式

IP 访问列表配置态

使用说明

可以使用访问表控制包在接口上的传输，控制虚拟终端线路访问以及限制路由选择更新的内容。在匹配发生以后停止检查扩展的访问表。分段 IP 包，而不是初始段，立即由任何扩展的 IP 访问表接收。扩展的访问表用于控制访问虚拟终端线路或限制路由选择更新的内容，不必匹配 TCP 源端口、服务值的类型或包的优先权。

注意：

在初始建立一个访问表后，任何后续的添加内容（可能由终端键入）放置在列表的尾部。

示例

下面示例禁止 192.168.5.0 这个网段：

```
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
```

注意：

IP 访问表由一个隐含的 deny 规则结束。

相关命令

ip access-group

ip access-list

permit

show ip access-list

1.1.2 ip access-group

为了控制访问一个接口, 使用 ip access-group 接口配置命令。为了删除这个指定的访问组，使用 no 格式命令。

ip access-group {*access-list-name*}

no ip access-group {*access-list-name*}

参数

参数	参数说明
access-list-name	访问表名。这是一个最长为20个字符的字符串。

命令模式

接口配置态

使用说明

访问列表用在入接口。对于标准的入口访问列表，在接收到包之后，对照访问列表检查包的源地址。对于扩展的访问列表，该交换机也检查目标地址。如果访问表允许该地址，那么软件继续处理该包。如果访问表不允许该地址，该软件放弃包并返回一个 ICMP 主机不可到达报文。

如果指定的访问列表不存在，所有的包允许通过。

示例

下例在以太网接口 10 的包出口上应用列表 filter：

```
interface g0/10
ip access-group filter
```

相关命令

ip access-list

show ip access-list

1.1.3 ip access-list

使用此命令后，进入的 IP 访问列表配置模式。在这状态下可以增加和删除访问规则。命令 exit 返回配置状态。

使用 no 前缀，删除 IP 访问列表。

ip access-list {**standard** | **extended**} *name*

no ip access-list {**standard** | **extended**} *name*

参数

参数	参数说明
standard	指定为标准访问列表。
extended	指定为扩展访问列表。
name	访问表名。这是一个最长20的字符串。

缺省

没有 IP 访问列表被定义。

命令模式

全局配置态

使用说明

使用此命令将进入 IP 访问列表配置模式，在 IP 访问列表配置模式中，可以用 deny 或 permit 命令来配置访问规则。

示例

以下的例子配置一个标准访问列表。

ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any

相关命令

deny

ip access-group

permit

show ip access-list

1.1.4 permit

在 IP 访问列表配置模式中可使用此命令配置允许规则，要从 IP 访问列表中删除 permit 规则，在命令前加 no 前缀。

permit source [*source-mask*]

no permit source *[source-mask*]

permit protocol source *source-mask* **destination** *destination-mask* [**tos** *tos*]

no permit protocol source *source-mask* **destination** *destination-mask* [**tos** *tos*]

对于互联网控制报文协议(ICMP)，也可以使用以下句法：

permit icmp source *source-mask* **destination** *destination-mask* [*icmp-type*] [**tos** *tos*]

对于 Internet 组管理协议(IGMP)，可以使用以下句法：

permit igmp source *source-mask* **destination** *destination-mask* [*igmp-type*] [**tos** *tos*]

对于 TCP，可以使用以下句法：

permit tcp source *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**tos** tos]

对于数据报协议(UDP)，可以使用以下句法：

permit udp source *source-mask* [**operator port** [*port*]] **destination** *destination-mask* [**tos** *tos*]

参数

参数	参数说明

protocol	协议名字或IP协议号。它可以是关键字icmp、igmp、igrp、ip、ospf、tcp或udp，也可以是表IP协议号的0到255的一个整数。为了匹配任何Internet协议(包括ICMP、TCP和UDP)使用关键字ip。某些协议允许进一步限定，如下描述。
source	源网络或主机号。有两种方法指定源：32位二进制数，用四个点隔开的十进制数表示。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
source-mask	源地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
destination	目标网络或主机号。有两种方法指定： 使用四个点隔开的十进制数表示的32位二进制数。 使用关键字any作为0.0.0.0 0.0.0.0的目标和目标掩码的缩写。
destination-mask	目标地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的目标地址和目标地址掩码缩写。
tos *tos*	(可选) 数据包可以使用服务层过滤。使用数字0－15指定。
icmp-type	(可选)ICMP包可由ICMP报文类型过滤。类型是数字0到255。
igmp-type	(可选)IGMP包可由IGMP报文类型或报文名过滤。 类型是0到15的数字。
operator	(可选)比较源或目标端口。操作包括eq(等于)。如果操作符放在source和source-mask之后，那么它必须匹配这个源端口。如果操作符放在destination和destination-mask之后，那么它必须匹配目标端口。
port	(可选)TCP或UDP端口的十进制数字或名称。端口号是一个0到65535的数字。

命令模式

IP 访问列表配置态

使用说明

可以使用访问表控制包在接口上的传输，控制虚拟终端线路访问以及限制路由选择更新的内容。在匹配发生以后停止检查扩展的访问表。

分段 IP 包，而不是初始段，立即由任何扩展的 IP 访问表接收。扩展的访问表用于控制访问虚拟终端线路或限制路由选择更新的内容，不必匹配 TCP 源端口、服务值的类型或包的优先权。

注意：

在初始建立一个访问表后，任何后续的添加内容(可能由终端键入)放置在列表的尾部。

示例

下面示例允许 192.168.5.0 这个网段：

```
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
```

注意：

IP 访问表由一个隐含的 deny 规则结束。

相关命令

deny

ip access-group

ip access-list

show ip access-list

1.1.5 show ip access-list

要显示当前的 IP 访问列表内容，使用 show ip access-list 命令。

show ip access-list[*access-list-name*]

参数

参数	参数说明
access-list-name	访问表名。这是一个最长20的字符串。

缺省

显示所有标准的和扩展的 IP 访问列表。

命令模式

管理态

使用说明

show ip access-list 命令允许你指定一个特定的访问列表。

示例

以下是不指定名时 show ip access-list 命令的示例输出：

```
Switch# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```

以下是指定访问表名时, show ip access-list 命令的示例输出：

```
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```